Federal Implementation Guidelines for Electronic Data Interchange (EDI)

Federal Government

Comment Version

July 2001

10.0 FEDERAL CONVENTIONS FOR USING ASC X12 TRANSACTION SETS

This part of the Guideline defines the federal transaction set conventions to be used when operating in the ASC X12 environment. It includes the instructions for implementing the control and security structures for batch EDI, and definitions of the usage indicators and applicable codes.

This version of Part 10 of the Guideline is based on the ASC X12 Standard, Version 004 Release 030 (004030). It supersedes and cancels all previous versions. To support existing EDI implementations, some of the individual Interchange Control Structure Implementation Conventions included in Part 10.6 will support previous versions of the ASC X12 Standard. Except where specifically indicated, this document defines how the agencies, components and activities of the United States federal government will exchange EDI data formatted in accordance with the provisions of the ASC X12 standards.

10.1 INTRODUCTION

The power of the ASC X12 standard is in its building block concept, which standardizes the essential elements of business transactions. The concept is similar to a "standard bill of material" and the "construction specifications", which give the architect flexibility in what can be designed with standardized material and procedures. The EDI system designer, like the architect, uses the ASC X12 standards to build business transactions that are often different because of their function and yet utilize the ASC X12 standards. The "bill of material" and the "construction specification" of ASC X12 are the standards found in the published technical documentation. The listing below identifies major parts of the published ASC X12 technical documentation:

- ASC X12.3, ***December 1999***. The *Data Element Dictionary* specifies the data elements used in the construction of the segments that comprise the transaction sets developed by ASC X12.

- ASC X12.5, ***December 1999***. The *Interchange Control Structure* provides the interchange control segment (also called an envelope), consisting of a header and trailer, for the EDI transmission; it also provides a structure to acknowledge the receipt and processing of the envelope.

- ASC X12.6, ***December 1999***. The *Application Control Structure* defines the basic control structures, syntax rules, and semantics of EDI.

- ASC X12.22, ***December 1999***. The *Data Segment Directory* provides the definitions and specifications of the segments used in the construction of transaction sets developed by ASC X12.

- ASC X12.58, ***December 1999***. The *Security Structures* define the data formats for authentication, encryption, and assurances in order to provide integrity, confidentiality, verification and non-repudiation of origin for two levels of exchange of EDI formatted data. Security structures may be applied at the functional group level or the transaction set level or both.

- ASC X12.59, ***December 1999***. The *Implementation of EDI Structure/Semantic Impact* provides a clear distinction between the syntax of ASC X12 structures and the semantics of transaction set usage.

- ASC X12C/TG1/95-65. *Technical Report Reference Model for the Acknowledgment and Tracking of EDI Interchanges* summarizes the use of the ASC X12 control elements and standards for the acknowledgment and tracking of EDI interchanges.

The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Recommendation X.509 (1993)/ ISO/IEC 9594-8 (1995), *Information Technology- Open Systems Interconnection- The directory: Authentication Framework* defines a framework for the provision of authentication services by the directory to its users. It specifies the form of authentication information held by the directory, describes how authentication information may be obtained from the directory, states the assumptions made about how authentication information is formed and placed in the directory, defines three ways in which applications may use authentication information to perform authentication, and describes how other security services may be supported by authentication.

The government translation function shown in the Acknowledgment Model in Section 10.4.1, can be implemented as part of the government AIS, as part of the DEBX, or as a stand-alone function. The government point of translation (GPoT) acknowledgment responsibility resides at the location performing translation. The requirement to provide acknowledgment transactions is a matter of agreement between partners. The GPoT retains the responsibility for providing acknowledgement information to the government transaction originator as agreed to by the partners involved. The vendor translation function can be implemented as part of the vendor application, Value Added Network (VAN), or as a stand-alone function.

In addition to using existing standards to build specific transactions, the standards may be used to provide control and tracking of interchanges if accomplished in a specific standardized approach. ASC X12 has defined and approved several control structures and transaction sets intended to augment EDI auditing and control systems. This Guideline provides a tracking mechanism for EDI data as it moves through the transmission cycle. Through the implementation of these tracking tools and analysis of the resulting information, delay or failures in delivery can be identified and corrected.

The work accomplished by The Communications and Controls Sub-committee (ASC X12C) in this area produced a generic acknowledgment model that has been adapted to support federal government EDI processes. Implementation of the acknowledgment mechanisms identified by this model will provide a basic capability to track interchanges as they flow from senders through service request handlers (SRH) to receivers across the EC/EDI Infrastructure.[1] This basic capability will provide functionality for each component to determine translation and transmission status, including current location and disposition of an interchange. Use of the implemented acknowledgment mechanisms to determine singular event status can provide components with the information necessary to obtain some level of confidence that interchanges are flowing through the infrastructure properly. Taken as a sequence of acknowledgment events, the model provides senders with a means to track interchanges from generation to delivery to a SRH at the boundary of the infrastructure. This tracking is accomplished without imposing the processing and communications overhead that would be required for true application-to-application acknowledgments. The implemented acknowledgment mechanisms of this model will allow individual components to build upon or enhance their internal audit trail processes.

This part of the Guideline is meant to be an overarching architecture of the control and security structure, which the government is implementing in the electronic commerce infrastructure (ECI), and other government EC activities. However, not all the parts of the architecture will be

[1] A SRH is a service provider whose primary function is to provide communications services between other components in the model.

implemented immediately. The specifics of which parts are actually implemented will be defined in agreements between actual components in the trading network and architecture, such as VANs and government users of the ECI.

This Guideline does not specify how to use the implemented acknowledgment mechanisms. While support of these mechanisms is required, their usage between infrastructure components will be as agreed to between those components. The use of certain acknowledgement mechanisms between the government and VANs and the gateways may be specified in an agreement(s) between the parties. When there is a conflict between this Guideline and any such agreement(s), this Guideline shall take precedence.

The acknowledgments used between the GPoT and other infrastructure components will be mutually agreed to by the respective parties. The exception to the above policy is when a pre-existing agreement specifically provides for deviation from the approved acknowledgment mechanisms in this Guideline. In those instances, the terms of the agreement shall take precedence.

By focusing on basic acknowledgment functionality, independent of communications protocols, enhanced tracking of interchanges is accomplished without requiring individual components to adhere to or support a full accountability system.

For further clarification of acronyms, abbreviations, and codes, refer to ASC X12 published technical documentation. For copies, contact the EDI focal point either within your service or agency, or, alternatively, contact the administering body (see Section 1.3 of this Guideline).

10.1.1 Year 2000 Compliant Date Formatting

Data elements reflecting dates in ASC X12 version/release 004010 and beyond are capable of carrying Year 2000 (Y2K) compliant dates in the standard date format (CCYYMMDD). While the use of 004010 and higher versions is the preferred alternative for becoming Year 2000 compliant, a methodology for distinguishing between the 20th and 21st centuries is necessary for earlier versions. For the purpose of Y2K compliance, the following are work-around and permanent solutions for meeting Y2K compliance.

10.1.1.1 Bridging (49/50 rule) is applicable for versions 2003-3070

Bridging is a technique in which a year of 00 – 49 is considered to reference the year 2000, and a year of 50 – 99 is considered to reference the 1900-year. This solution requires that the AIS make modifications to decipher the bridging schemes. If necessary, systems that employ a "bridging" scheme will need to identify ICs that are impacted and provide additional implementation notes on the usage of the bridging scheme.

Note: The bridging solution is the only option available for systems based on versions 002003–003010; these versions of the ASC X12 Standard do not support the century date format.

Examples of bridging using the 6-digit date format to depict the century. [**YY**MMDD]

1. 19[**50****1206**] = 1950 December 06
   YYMMDD

3. 19[**59****1206**] = 1959 December 06
   YYMMDD

4. 20[**00****1206**] = 2000 December 06
   YYMMDD

5. 20[**49****1206**] = 2049 December 06
   YYMMDD

10.1.1.2 Date & Century Data Elements is applicable for versions 003020–003070.

Use data element 373 [Date YYMMDD] in conjunction with data element 624 [Century CC].

Use data element 1250 [Date Qualifier CC] in conjunction with data element 1251 [Date Time Period].
Note: Systems based on versions 003020–003070 can either use the bridging solution or composite date solutions (DATA ELEMENT 373 and DATA ELEMENT 624) or (DATA ELEMENT 1250 and 1251) for Y2K compliance. If the ICs impacted do not support the composite date solutions (i.e. DATA ELEMENT 373 or 1250 marked "Not Used"), then the bridging solution is appropriate.

10.2 CONTROL SEGMENTS

In addition to communications control, the EDI interchange structure provides the standards user with multiple levels of control to ensure data integrity. It does so by using header and trailer control segments designed to uniquely identify the start and end of the interchange, functional groups and transaction sets. Figure 10-1 shows the relationship of these control segments. Section 10.6 defines Control Segment specifications. Envelope control segments have few options and, except for minor tailoring, are identical for every EDI interchange.

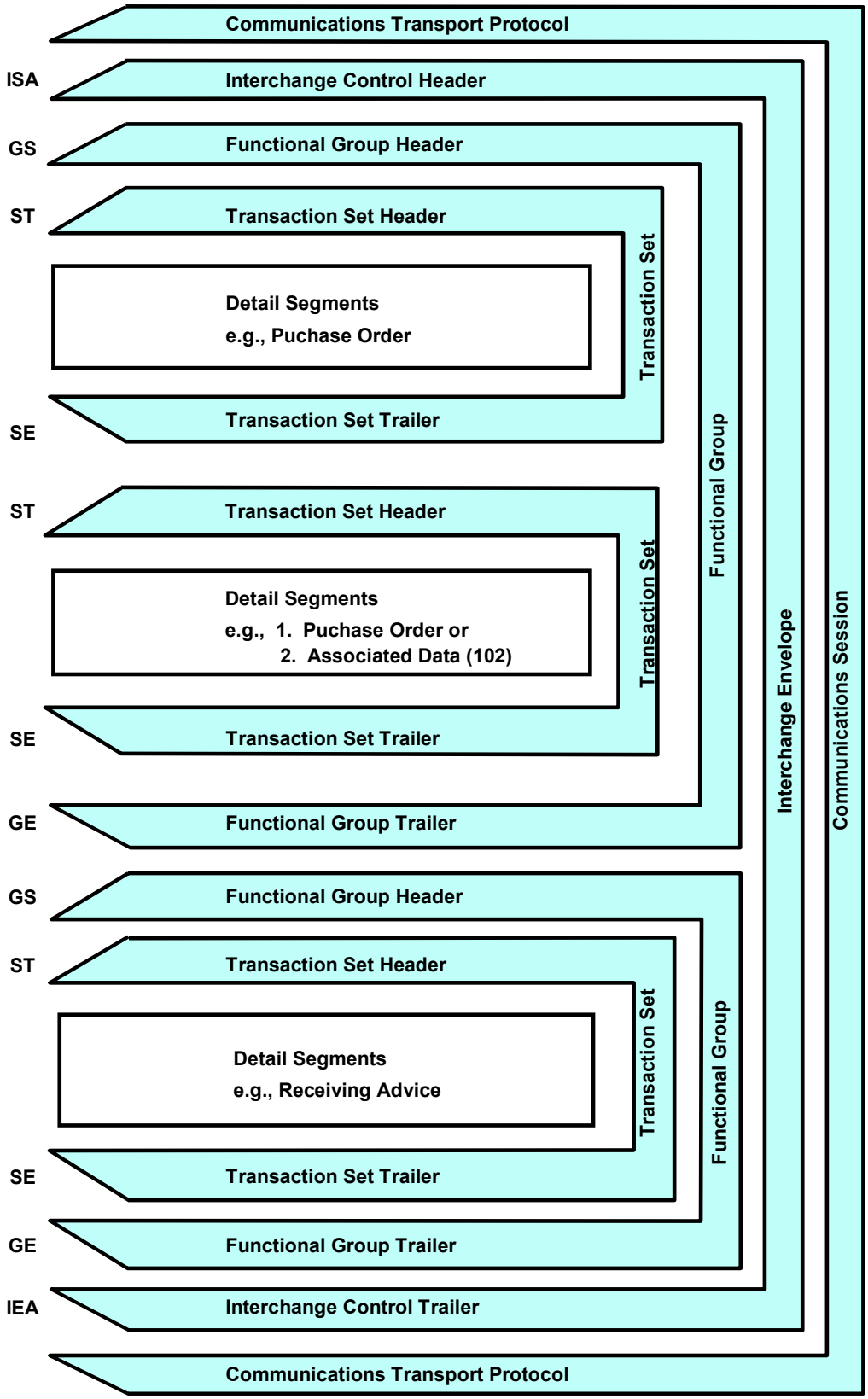
10.2.1 Description of Use

The interchange header and trailer segments (ISA/IEA) along with the optional interchange acknowledgment segments (TA1 - Interchange Acknowledgment and TA3 - Interchange Delivery Notice) constitute the interchange control structure (i.e., an interchange envelope) as defined in the ASC X12 standard. **The federal government acknowledgment model does not use the TA1 segment**. Interchange control segments perform the following functions:

- Define data element separators, sub-element separators, repetition separators, and data segment terminators
- Provide control information
- Identify interchange sender and receiver
- Provide capability for authorization and security information.

The actual interchange control structure includes neither the group control structures nor the transaction control structures. ASC X12 defines these as application control structures, and their version and release may differ from those for the interchange envelope. An interchange envelope encompasses one or more functional groups (GS/GE), which, in turn, enclose one or more transaction sets (ST/SE). The relationship for these structures is illustrated in Figure 10-1.
The GS/GE functional grouping provides an additional control envelope surrounding like transaction sets conforming to a unique IC or for ASC X12 version and release transaction sets conforming to the same version and release. Their usage is prescribed as interchange control segments in order to present a consistent methodology for EDI within the federal government community and for commercial entities that conduct EDI business with the federal government.

Figure 10 -1. Hierarchical Structure



Note: When an Interchange contains TA3s, it shall contain only TA3s. The TA3s replace all Functional Groups, Security Envelopes, Transaction Headers and Trailers, as well as Detail Segments in the above diagram.

10.2.1.1 DATA ELEMENT, DATA SEGMENT, COMPONENT DATA ELEMENT SEPARATION, AND REPETITION SEPARATION

In ASC X12 documentation, the data element separator is graphically displayed as an asterisk (*). The actual data element separator employed within the interchange envelope dictates the value for the entire interchange. The first occurrence of the data element separator is at the fourth byte of the interchange control header. The value appearing there dictates the data element separator used through the next interchange trailer.

In a similar manner, the interchange control header establishes the value to be used for segment termination within an interchange. ASC X12 documentation represents this graphically by a new line (N/L). Note: the federal government uses the tilde (~) to represent segment termination. The first instance of segment termination occurs immediately following the ISA16 data element, and the data value occurring there sets the value for the interchange.

Unlike the data element separator and the segment terminator, the other two delimiters are identified in the ISA segment by a discrete element. The value of the component data element separator is defined in element position (ISA16) and is graphically represented by the back slash (\). The repetition separator value is defined in element position (ISA11) and graphically represented by the back quote (`). It is used to identify the repetition of a simple data element or a composite data structure.

Table 10- 1. Federal Government Service Characters

Functionality	ASCII Hexadecimal	Graphic Representation	Name
Data element separator	1D	*	Asterisk
Segment terminator	1C	~	Tilde
Component data element separator	1F	\	Back slash
Repetition separator	1E	`	Back quote

These characters are reserved for these purposes and shall not be used in data elements, except that they may be used in binary data. Binary data is always transmitted in data element 785, Binary Data. The federal government ECI shall send and receive textual data ASCII encoded. If unencrypted binary segments are filtered, Base 64 filtering shall be used.

10.2.1.2 IDENTIFICATION OF IMPLEMENTATION CONVENTION

Section 10.6 contains Implementation Conventions (ICs) for ASC X12 Version 004020 and later. It also contains ICs to support implementations for ASC X12 Version 004010 and earlier.

10.2.1.2.1 Version 004010 and Earlier

Implementation Conventions (ICs) for using the ASC X12 interchange control structures are provided in Section 10.6. To document a consistent approach to control structure content .The functional group control structures include the ability to identify specific ICs to which the transaction sets contained within that group conform.

Interchange senders will provide the ASC X12 Version/ Release/Sub-release and IC identifier in GS08. This identifier uniquely identifies the IC to which the transaction set conforms. The GS ICs in Section 10.6 provide specific details and examples of the data string used to identify the specific IC that applies to the transactions contained within the group.

10.2.1.2.2 Version 004020 and Later ASC X12 version 004020 introduced a new methodology for referencing an IC within the interchange. The transaction set header added data element 1705 at position ST03 (Implementation Convention Reference). The IC unique identifier data to which the transaction set conforms is specified as a data string in ST03. The principal reason is to enable linked data sets, such as an 840 Transaction Set (Request for Quotation) with a matching 102 Transaction Set (Associated Data) to be contained within the same functional group. Previously, the 102 Transaction Set could only be sent in separate functional groups or separate transaction sets. Now, any of the three methods may be used.
This capability removes an existing restriction that requires transaction sets sent within a functional group to reference the same IC. The ST IC in Section 10.6 provides specific details and examples of the data string used to identify individual ICs.
Translators will reference the IC identifier at GS08 for the functional group, first. If the ST03 lists a different IC, the IC listed in GS08 will be over-ridden for that specific transaction set.

10.2.1.3 CONTROL NUMBERS

ASC X12 standards provide for syntax control on three levels: interchange, group, and transaction. Within each level, control numbers must exhibit a positive match between the header segment and its corresponding trailer (i.e., ISA/IEA, GS/GE, and ST/SE). This match provides a means to detect loss of data. Assignment of these control numbers, at each level, is as follows:

- ISA/IEA—Interchange Control Number:

➢ The nine-digit interchange control number is usually assigned by the originator's translation software. Originating organizations may use any numbering scheme consistent with their business practice. The scheme must provide sufficient uniqueness to identify each interchange. Unique identification is defined as the triplet: Interchange Sender ID, (ISA05, ISA06), the Interchange Receiver ID, (ISA07, ISA08) and the Interchange Control Number (ISA13). This triplet shall be unique within a reasonably extended time frame, such as a year. The ISA/IEA Interchange Control Number (ISA13/IEA02) is detailed in the IC in Section 10.6.

- GS/GE—Group Control Number (GS06/GE02):

➢ The one to nine digit Group Control Number is usually assigned by the originator's translation software. The scheme must provide sufficient uniqueness to identify each functional group transmitted between sending and receiving application pairs. Originating organizations may use any numbering scheme consistent with their business practices.

➢ The Group Control Number value (GS06), together with the application sender's code (GS02), Application Receiver's Code (GS03), and Functional Identifier Code (GS01), shall be unique within an extended time frame, such as a year. The GS/GE Group Control Number (GS06/GE02) is detailed in the applicable version/release ICs in Section 10.6.

- ST/SE Transaction Set Control Number

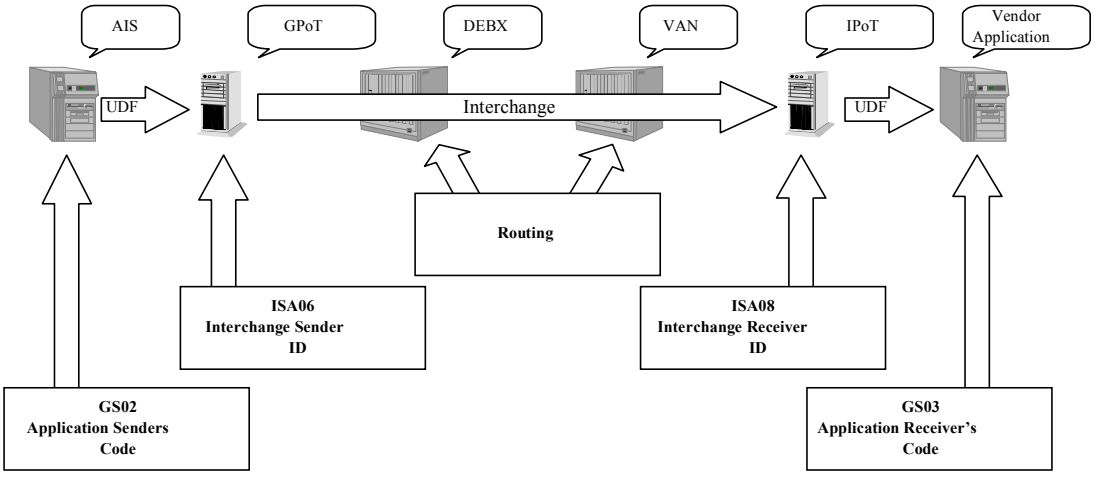
➢ The one- to nine-digit Transaction Set Control Number is usually assigned by the originator's translation software. Originating organizations may use

any numbering scheme consistent with their business practices, however the control numbers within corresponding header and trailer segments must uniquely identify each transaction set, within the context of the Functional Group. This control number provides a means to detect loss of data. The ST/SE Transaction Set Control Number (ST02 and SE02) is detailed in the IC found in Section 10.6.

10.3 ADDRESSING

The purpose of addressing is to provide an explicit reference to a transmission's sender and intended receiver. The addressing model used by the federal government for ASC X12 EDI transmissions is graphically depicted in Figure 10.2. In this model, there is addressing for two types of transmissions. The first is an interchange, it consists of control segments and application data. The second type is business application data that flows from the sender to receiving applications and is transported within an interchange. Since interchanges are assembled by the sending translation point and disassembled by the receiving translation point, the flow of an interchange is defined to be from translation point to translation point. Business application data must be provided to the sending translation point by the sending application and is depicted as a User Defined File (UDF). It must also be provided to the receiving application by the receiving translation point and is also depicted as a UDF. While the model depicts data flow from the government to a vendor, it is equally applicable in the reverse flow.

Figure 10-2. Addressing Model



GPoT = Government Point of Translation
IPoT = Industry Point of Translation

10.3.1 Interchanges

ASC X12 interchanges flow between translation locations. The GPoT can be implemented as part of the government AIS, as part of the DEBX, or as a stand-alone function. Likewise, the IPoT on the vendor side can be in the vendor application, as part of the VAN services, or as a stand-alone function.

All commercial and government entities conducting business electronically under this guideline shall provide their translation point (ISA06/ISA08) codes during registration. The GPoT and IPoT are addressed by the Interchange Sender ID (ISA05 and ISA06) and Interchange Receiver ID (ISA07 and ISA08) data elements. Translation Points (ISA06 and ISA08) shall be identified via a

unique identifier from one of the sources listed as allowable codes in the ISA05/ISA07 definition in Section 10.6.
When an interchange contains one-to-one transactions, the Interchange Sender ID (ISA06) and Interchange Receiver ID (ISA08) data elements shall be the addresses of the interchange translation points (both government and non-government). D-U-N-S number and D-U-N-S+4 are the preferred identifiers (additional identifiers are indicated in the ISA IC found in Section 10.6). These, combined with the Interchange Control Number (ISA13), create a triplet that defines a globally unique identifier for the interchange. The ASC X12 Interchange flows between these translation points. In the ECI, when an interchange contains "PUBLIC" transactions the ISA08 will be addressed individually to all VANs registered to receive those transactions. The ISA06 will contain the DEBX address.

10.3.2 Application Sender and Receiver Codes

Application data is transported within the interchange via groups. Group addressing (GS02/GS03) must define the user application end points shown in Figure 10.2 as the AIS and the Vendor Application. These addresses are locally unique and are defined between the translation point and its customers. Data that flow between the translation points and the Application Senders and Receivers are not defined by ASC X12, but are in a format agreed upon between the applications and their translation points.
ASC X12 standards provide for the identification of senders and receivers on two levels, the interchange and the group. The group level identifies application senders and receivers. Depending on where translation is performed, the sender/receiver IDs may be the same at the interchange and group levels and may use any number of available naming schemes. The GS02/03 identifiers need be unique only within the context of the associated ISA address. All commercial and government entities conducting business electronically shall provide their Application Sender and Receiver (GS02/GS03) codes during the Central Contractor Registration process.
The D-U-N-S and D-U-N-S+4 are recommended for use at the GS/GE level, especially for identifying government organizations. Other identifiers listed in the IC may be used.
A D-U-N-S number may be acquired from Dun and Bradstreet and the plus 4 portion of the number is assigned and maintained internally by each entity. Specific use of these numbers is provided for in the Control Structure section of this guideline.

10.4 ACKNOWLEDGMENTS

The successful conduct of business via EDI requires that trading partners know when transactions were received, not received, received in error, or otherwise did not complete the communications or receiver application processing cycle. The generation or handling of these events may be communications based, EDI processing based, or both. Additionally, senders may desire to know such information on an exception basis, such as reporting only for error conditions, or they may need regular indication of the delivery status to maintain local, internal audit information. Communication services providers may need to know when interchanges for which they have accepted responsibility were forwarded and accepted by the next service provider in the transmission path, or whether forwarding was not successful.
Transmission or processing of interchanges can be viewed as an acknowledgment event in a general sense, creating the need for some response. From a sender's perspective, the acceptance of their interchange by a translator or communications provider is an acknowledgment event that could either be indicated by a simple receipt, or a more robust reporting of what actions were taken after receipt. For a service provider, forwarding interchanges can also result in an acknowledgment event being created that calls for an acknowledgment action to take place. Taken as a set of acknowledgment requirements, these and other events can be considered as a set of circumstances, which result in or require some acknowledgment action to take place. Rather than consider every possible action and event, a basic sub-set of these events can be defined to describe the majority of cases and form a generalized picture of tracking interchanges. Together with acknowledgment mechanisms that relate to those events and specific components that create or respond to those events, an acknowledgment model can be described.

ASC X12C produced a generic Acknowledgments Model in X12C/TG1/98-172 -- *Reference Model for the Acknowledgment and Tracking of EDI Interchanges*. This technical report identifies specific entities in the EDI communications and processing path that serve as the event generators or handlers, as well as identifying ASC X12 standards based acknowledgment mechanisms. Also, the senders and receivers of the interchanges are recognized as being the terminating application systems for which the EDI transactions are sent from or sent to, regardless of where translation occurs.

The federal government adapted the ASC X12 approach to an acknowledgment model, and refined it through identification of specific entities and acknowledgment events. Support for this model provides users and service providers with the ability to track interchanges and respond to requests for status of such interchanges. In addition, the internal audit trail processes of each entity will be enhanced with the availability of specified event mapping.

10.4.1 Acknowledgment Model Description

As adapted from the generic model developed within ASC X12C, the government acknowledgment model identifies specific components, acknowledgment events, and ASC X12 mechanisms that are related to those events. Based upon the DEBX as a central component, the model establishes a view of the EC/EDI infrastructure as encompassing commercial and government entities, as well as service providers and users.

In this model, a service request handler (SRH) acts as a service provider for translation services, communications services, or some EDI processing services. Specifically, the model identifies the DEBX, VAN and translation point as service providers whose primary function is to provide communications services between other components in the model. Users include trading partners (TPs) and Automated Information Systems (AISs).

The acknowledgment mechanisms identified in the model include unspecified as well as ASC X12 based mechanisms. Where the model has identified an acknowledgment event but does not specify a mechanism for handling that event, it is implied that components involved in that event will agree on the mechanism to be used.

ASC X12 based acknowledgment mechanisms include control segment structures and transaction sets. The Interchange Delivery Notice (TA3) segment, Data Status Tracking (242) transaction set and the Functional Acknowledgment (997) transaction set all have distinct properties and functions. However, their use in a general sense as acknowledgment mechanisms allows a sequence of communications and processing events to be tied together in a logical stream. Each acknowledgment event is mapped to an ASC X12 standards based mechanism according to where the event takes place, what type of event occurred, and what role the receiving or generating component plays in the data flow stream.

The TA3 can provide information on the status of delivery of an interchange, the time an interchange was received, or the disposition of an interchange, and is used to report such information between SRHs.The Data Status Tracking (242) transaction set, in addition to providing the ability to represent the information contained in the TA3, allows transmission status information to be conveyed from SRHs to senders. The Functional Acknowledgment (997) transaction set indicates the status of translation of the interchange header and trailer information. These mechanisms are described in more detail later in this section.

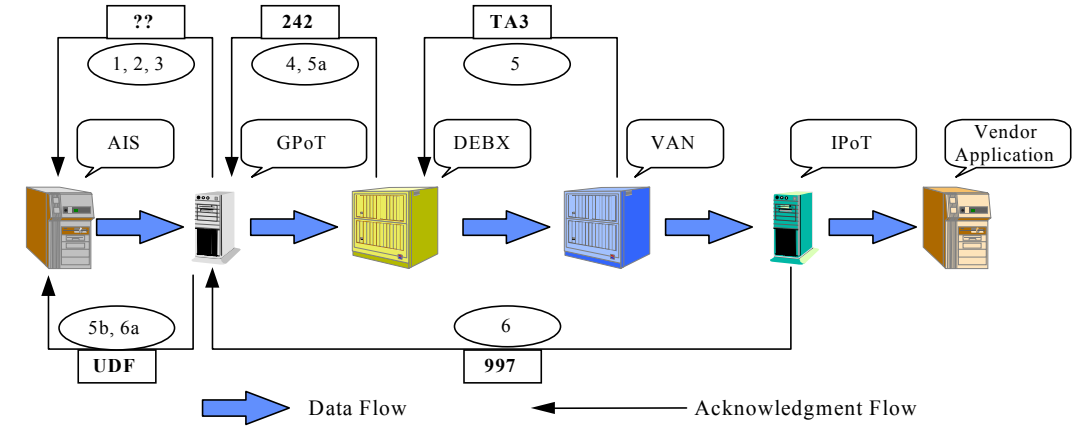
The government translation function shown in the acknowledgment model can be implemented as part of the government AIS, as part of the DEBX, or as a stand-alone function. The GPoT acknowledgment responsibilities reside at the location performing translation. The vendor translation function can be implemented as part of the vendor application, VAN or as a stand-alone function. The IPoT acknowledgment responsibilities reside at the location performing translation.

The acknowledgement model depicted in Figures 10-3 and 10-4, and Tables 10-2 and 10-3, identifies the set of events that, through implementation and use of the specified acknowledgment mechanisms, provides for the tracking of interchanges across the infrastructure. The specifics of which acknowledgement mechanisms are actually implemented will be defined in agreements between actual components in the trading network and architecture, such as VANs and government users of the ECI.

Note: Use of the Functional Acknowledgment is encouraged however; do not transmit the Functional Acknowledgment unless mutually agreed to by <u>both</u> trading partners. For clarity in the illustration and discussion, usage of the Functional Acknowledgment and other acknowledgement mechanisms is assumed.

The acknowledgement model identifies the requirement for acknowledgments from a GPoT to supported government AISs, though no single acknowledgement mechanism is prescribed. When a Functional Acknowledgment is required by the parties involved, the recommended technique is to pass the Functional Acknowledgement data, as defined by the sender (e.g., AIS), from the GPoT to the AIS using a methodology and technology (e.g., email, telephone, flat file exchange, etc.) as agreed to by the parties involved. Paragraph 10.4.3 includes additional discussion of this subject.

Figure 10-3. Acknowledgment Model, Commercial to Government



Notes:
a. The GPoT translation function may be performed by the DEBX AIS, or by a separate entity.
b. For the purposes of the model, the govt-to-govt scenario is represented by replacing the VAN-Translation components with a GPoT component.
c. The IPoT may be operated by the VAN, the Vendor, or a third party. In all cases, the IPoT is the ultimate recipient of the interchange for the purposes of acknowledgment in this model.
d. 997s and 242s can be converted at the GPoT to information formats and forwarded to the AIS as agreed between and the sender. 242s will not be acknowledged by 997s.
e. UDF is User Defined File (flat file, proprietary file).
f. The use of 824s are not precluded by this model.
g. Support for the model acknowledgment mechanisms is mandatory. The manner of their usage is as detailed further in this Guideline and agreements between components.

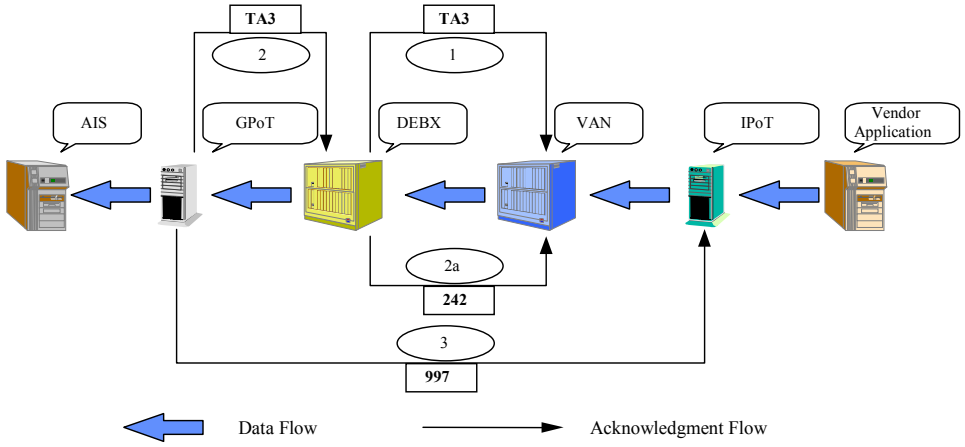
Table 10-2. Acknowledged Events, Commercial to Government

Sequence/Event	Mechanism	From	To
1. Receipt of UDF by GPoT	TBD	GPoT	AIS
2. Translation Result	TBD	GPoT	AIS
3. Disposition (Acknowledge that interchange has left GPoT)	TBD	GPoT	AIS
4. Interchange receipt by DEBX	242	DEBX	GPoT
5. Interchange Disposition at SRH (Government to Government)	TA3 TA3	VAN GPoT	DEBX DEBX
5a. Report of Interchange Disposition at SRH	242	DEBX	GPoT

5b. Report of Interchange Disposition at SRH	UDF	GPoT	AIS
6. Translation Result	997	IPoT	GPoT
6a. Translation Result	UDF	GPoT	AIS

Notes: Not all events 1, 2, or 3 may occur or need to be acknowledged; TBD indicates the acknowledgment mechanism is to be determined, or as agreed to between the parties; UDF: User Defined File (flat file, proprietary file format).

Figure 10-4. Acknowledgment Model, Government to Commercial



Notes:
a. Acknowledgments among VANs, Translation Points and their customers are matters to be decided by them and are not defined in the government Acknowledgment Model.
b. Some GPoTs may generate a second 242, with the DEBX acting as a pass-through.
c. For government to government scenario, replace the VAN with a GPoT. The DEBX will generate 242s in lieu of TA3s in step 1.

Table 10-3. Acknowledged Events, Government to Commercial

Sequence/Event	Mechanism	From	To
1. Interchange receipt by DEBX (Government to Government)	TA3	DEBX	VAN
	TA3	DEBX	GPoT
2. Interchange Disposition at GPoT	TA3	GPoT	DEBX
2a. Report of Interchange Disposition at GPoT (Government to Government)	242	DEBX	VAN
	242	DEBX	GPoT
3. Translation Result	997	GPoT	IPoT

Notes: Not all events 1, 2 or 3 may occur or need to be acknowledged; UDF: User Defined File (flat file, proprietary file format).

10.4.2 Interchange Acknowledgment

At the interchange level, acknowledgments can occur for a number of events. Successful translation, syntax error, or a more detailed acknowledgment of the disposition of an interchange can be reported. The available ASC X12 mechanisms for such interchange acknowledgments include the Functional Acknowledgment (997) transaction set, the Interchange Acknowledgment Segment (TA1), and the Interchange Delivery Notice Segment (TA3). **The TA1 is not supported**

in the federal government acknowledgment model implementation. [2] In general, the 997 is used exclusively for reporting the status of syntactical analysis of the interchange by the receiving translator, although it could be used as an indication that an interchange was received. The Interchange Delivery Notice (TA3) provides the ability for reporting on the status of actions taken on a particular interchange. The manner in which these mechanisms are used, and the features within each that are utilized, provides a set of tools for building a sequence of acknowledgments for the life cycle of an interchange as it flows across the ECI. The specifics of which acknowledgement mechanisms are actually implemented will be defined in agreements between actual components in the trading network and architecture, such as VANs and government users of the ECI. To ensure clarity in the discussion of the acknowledgement mechanisms, the discussion assumes they are being used.

10.4.2.1 TA3

The TA3 provides a notice from the receiving SRH to the sending SRH that an interchange was delivered, not delivered, refused, purged, or transferred to the next SRH. It provides a notification of action taken, notice of time/date action was taken, and the ability to report on more than one event.

As an acknowledgment mechanism in this model, the TA3 is used between the DEBX and VANs, acting as SRHs, to indicate the status of interchanges sent from the government to commercial components, as well as the reverse scenario. To indicate outbound delivery status, the information contained in this TA3 is further translated into a 242 transaction set and sent to GPoTs for their use, which may include supplying this information to the interchange sender. The government uses the TA3 to indicate interchange delivery status to the sending commercial infrastructure components.

Upon delivery of an interchange to the interchange receiver's mailbox, a TA3 shall be generated.
If delivery of the interchange to the interchange receiver's mailbox is not made within 2 hours, a TA3 shall be generated indicating a non-delivery status. The appropriate reason codes will be specified. A TA3 shall be generated every 2 hours indicating non-delivery status until the interchange is delivered to the receiver's mailbox.
Single or multiple TA3s may be sent in an interchange, however an interchange that contains a TA3 shall contain only TA3s. No acknowledgment is made for the receipt of a TA3. If an interchange is accepted but subsequently determined to be non-deliverable, a TA3 shall be generated indicating the reason.
If the TA3 is not received within 2 hours after an interchange was sent, then retransmit the interchange with the same interchange control number (ISA13). If an interchange is rejected, the corrected interchange shall have a new interchange control number (ISA13).

10.4.2.2 DATA STATUS TRACKING (242) TRANSACTION SET

The Data Status Tracking (242) transaction set conveys status information from a SRH, to the interchange sender, interchange receiver, or both. It can also be used to provide status information regarding an interchange as it flows from an interchange sender through one or more SRHs to an interchange receiver during its transmission cycle.

In the acknowledgment model, the 242 transaction set is used for two events:

1. It conveys information from the TA3 that was generated by the VAN or GPoT that received the interchange.

[2] The TA1 Segment duplicates much of the function of the Functional Acknowledgment Transaction (997) and was eliminated from the model in an earlier version of the Federal Guideline.

2. It provides acknowledgment information between government components. Because it is a transaction set, translation sites can map that information into a UDF for the sending application's use. Usage of this information depends on the internal business processes at the application site, and is not covered by the model. In addition, the GPoT may use this information in its capacity as a SRH for internal audit trail purposes.

For interchanges between government components, a 242 shall be generated upon delivery to the interchange receiver's mailbox. If delivery to the interchange receiver's mailbox is not made within 2 hours, a 242 shall be generated indicating a non-delivery status. The 242 transaction set shall not be acknowledged (via a 997), nor shall it be used to report the final disposition of a 997 transaction set. Additional 242 acknowledgments from interconnected service providers may be required by additional agreements among trading partners.

10.4.2.3 INTERCHANGE ACKNOWLEDGMENT SEGMENT (TA1)

The interchange acknowledgment segment (TA1) reports the status of processing a received interchange header and trailer or the non-delivery by a network provider. **The TA1 is not supported in the federal government acknowledgment model implementation.**

10.4.3 Functional Acknowledgment Methodology

There are two aspects of the government functional acknowledgement model. The first being the traditional use of the Functional Acknowledgement in the acknowledgement model business cycle. The second reflects a less well-defined and unstructured process of returning the Functional Acknowledgement information from the GPoT to the government AIS when these roles are preformed at separate entities.

10.4.3.1 FUNCTIONAL ACKNOWLEDGMENT USE IN THE ACKNOWLEDGEMENT MODEL

The Functional Acknowledgment is integral to the overall ECI process to ensure interchange integrity, and for completeness of the acknowledgment model even though it is not part of the interchange control structure. The Functional Acknowledgement supports three types of acknowledgments:

1. Receipt acknowledgement.
2. Acceptance of a functional group and the transactions contained within it based on EDI translation software syntax edits with respect to the ASC X12 standard.
3. Rejection of a functional group and the transactions contained within it based on EDI translation software syntax edits with respect to the ASC X12 standard.

Use of the Functional Acknowledgment is encouraged but is not mandated. The Functional Acknowledgment will not be transmitted unless mutually agreed to by both trading partners. **The Functional Acknowledgement will NOT report syntactical correctness by comparison to the requirements of the applicable IC.** If the Functional Acknowledgment is not used, the sender will not receive acceptance or rejection notification based on the EDI translation software syntax edits. Do not acknowledge a Functional Acknowledgement transaction set.

10.4.3.2 ACKNOWLEDGEMENT BETWEEN GPOT AND AIS

The Acknowledgement Model description contained in Figure 10-3 does not identify a specific acknowledgement mechanism for use between the GPoT and the AIS. There are three considerations for determining the specific acknowledgement mechanism.

1. The GPoT and AIS entity must agree to the types of Functional Acknowledgements to be exchanged.
2. The methodology of exchange (e.g., UDF) within a series of technologies (e-mail, phone, etc.) will be as defined by the GPoT and agreed to by the AIS.

3. The level of detail and actual data to be contained will be agreed upon between the parties.

10.4.4 Application Advice (824) Transaction Set

Although it can provide acknowledgment functionality, this model does not specify use of the Application Advice (824) transaction set. Full use of the 824 as an acknowledgment mechanism within the model would create substantial impact on the communications and processing systems. Currently, it is primarily used on an exception basis for reporting the results of business application system's data content edits of a transaction set. This could also include checking for compliance within the IC.

Note: The DEBX is not liable for the unsuccessful transmission of EDI transactions for those trading partners who opt not to implement a 997 or 824.

10.5 SECURITY

ASC X12.58, published in December 1997, provides for the implementation of security services at the functional group and transaction set levels for ASC X12 version 4010. The available security services include data integrity, confidentiality, assurance, verification, and non-repudiation of origin. These services may be implemented individually or in any combination.
ASC X12.58 can meet several security objectives. Among these are:

- The recipient of an EDI transaction can verify the identity of the originator of the transaction.
- The recipient of an EDI transaction can verify the integrity of its contents.
- The originator of an EDI transaction can provide confidentiality for its contents.

ASC X12.58 provides a mechanism that can be applied to the ASC X12 functional group or transaction set, in contrast to other alternatives which are usually applied to the entire interchange. ASC X12.58 is transaction data independent. When ASC X12.58 security mechanisms are applied inside the interchange, they can be handled and routed as standard ASC X12 transactions without disrupting the end-to-end security. Since security services are applied within the interchange, they are independent of the mechanism used to transport them. Thus, ASC X12.58 can provide security even when the interchanges leave the boundaries of the ECI.

The federal government is committed to providing security services for ASC X12 compliant EDI via the constructs provided by ASC X12.58. However, very significant changes to those constructs have been made within various version/releases of the ASC X12 standards. Also, ASC X12.58 security constructs are not backward compatible. That is, 4010 constructs may not be applied to provide security services to the bulk of the current federal implementations, which are in version/release 3070, 3060, 3050, 3040 and earlier. Due to the evolutionary development of security structures to support ASC X12 interchanges, the federal government has determined that it will not support security structures prior to version/release 3070.

10.5.1 Authentication

Message authentication is a procedure to verify that received messages have not been altered. A hash function, a public function that maps a message of any length into a fixed

hash value, can be used as an authenticator when used in conjunction with some form of data encryption, such as digital signature.

Implementation Note: Assurance via the S4A/SVA segments shall be used in lieu of authentication. For 3070 implementations, assurance via the S2A/SVA shall be used.

10.5.2 Confidentiality (Encryption)

The ASC X12.58 standards allow for the implementation of various algorithms to encrypt ASC X12 transactions. Cryptographic algorithms fall into two categories: secret key and public-key. Secret key algorithms are based on both the sender and receiver sharing the same secret key (i.e., key unknown to other parties). This key is used to encrypt the transaction prior to transmission and decrypt it upon receipt. Public-key algorithms are based on both sender and receiver having a pair of keys, one public and one private. All exchanges of keys between sender and receiver are limited to the public portion only, so the private key portion is protected. Confidentiality services may be applied at either the functional group (GS/GE) level, the transaction set (ST/SE) lever, or both. Initially, the government will support the following encryption algorithms:

- Data Encryption Standard (DES)
- Triple DES (DE3)
- Rivest-Shamir-Adleman (RSA)
- SKIPJACK

10.5.3 Assurance (Digital Signatures)

A digital signature is an authentication technique that also includes measures to counter repudiation by the source. Assurances as defined in ASC X12.58, allow the originator of the transaction to express "business intent" via a digital signature. Assurance (digital signature) may be applied at either the functional group (GS/GE) level, the transactions set (ST/SE) level, or both. The Government will support implementation of the Digital Signature Standard. When used, assurances are applied before any other security processes. For example, when both assurance and confidentiality are applied first and then confidentiality (S3S and S3E or S4S and S4E). In version 4010, the location of the group level assurance header segment (S3A) was changed. The S3A immediately follows the GS segment. The Security Value (SVA) segment follows any existing SVA segments and precedes the GE segment. This allows for efficient processing of the assurance segments. At the transaction level, the S4A segment replaces the S2A segment. The sequence of segments is detailed in Section 10.5.6.
For 3070 implementations, one S2A and one SVA are inserted immediately before the SE segment of the transaction set being assured. If subsequent assurances are applied, additional S2A/SVA pairs are inserted between the previous assurance, and the SE segment of the transaction set being assured. Detailed instructions for the use of the assurance segments are contained in section 10.6

10.5.4 ASC X12.58 Capabilities by Release

While the 004020 version of X12.58 reflects modifications of the security structure, data element 1621 (security version/release identifier) contains only a single code "004010". Until additional codes for further version/releases are added to the standard, the federal government security structure will remain at the 004010 level.
The following table reflects the capabilities provided by the ASC X12.58 standard. For implementation of these capabilities, reference the security structures in section 10.6.

Table 10-4. Capabilities Provided by ASC X12.58 Standard

ASC X12 Release	Authentication	Encryption	Assurance
3040	(Note 1)	(Note 3)	
3050	(Note 1)	(Note 3)	
3060	(Note 2)	X	X
3070	(Note 2)	X	X
4010	(Note 2)	X	(Note 4)
4020	(Note 2)	X	(Note 4)
4030	(Note 2)	X	(Note 4)

Notes: (1) Authentication accomplished using a message authentication code (MAC). The MAC is a hash of the data; (2) Authentication accomplished as a by-product of the digital signature or by using the MAC defined in earlier releases of the ASC X12 standard; (3) Private (symmetric) keys supported by this release. Asymmetric keying is possible but not without some "non-standard" use of data elements; and (4) The assurance capability is applied via the S3A or S4A and SVA segments.

10.5.5 Sequencing of Cryptographic Techniques

In practical situations, the users of the ASC X12.58 standards will choose combinations of features rather than just a single feature. This is possible since all features are designed to be used in isolation or in any combination.

Authentication does not protect the confidentiality of the message because the information is interchanged in its plain text form. Message encryption can be used to provide confidentiality while using authentication to provide integrity protection of the same data. When both authentication and encryption are used, the authentication is performed before encryption of the original plain text data.

Where more than one service is selected at a specific level, the order of processing is:

a) Before applying any security services, the data must first be translated into an EDI format
b) Addition of one or more assurances
c) Authentication
d) Compression
e) Encryption
f) Filtering for data communications

When assurance segments are used, they must be added to unsecured (not authenticated or encrypted) transactions. If a transaction set is received (with or without assurances) with encryption and/or authentication applied by the originator, the transaction set must be either decrypted or authenticated prior to the addition of any further assurances. Once any assurances have been added, the transaction set can be encrypted or authenticated prior to being forwarded to additional parties.

When applying security services at the functional group level, all security services at the transaction set level must be completed before applying security services at the functional group level.

The receiving organization processes the received message in the reverse order, starting with inverse filtering, followed by decryption, and then by decompression, validation of authentication and validation of the assurances. When processing inbound security services at the transaction set level, all security services at the functional group level must be removed before processing inbound security services at the transaction set level. In this manner the receiving organization unwraps the EDI message by processing the security services and removing the security segment pairs from the message before processing the next security service.

10.5.6 Transmission of Security Segments

Security services (authentication, encryption and assurances) are provided at two levels within ASC X12 in conjunction with the following envelopes:

- Functional Group (GS/GE envelope)
- Transaction Set (ST/SE envelope)

At each of these levels, authentication, encryption and assurances are each optional. Assurances are independent of authentication or encryption. In addition, any service used at one level is independent of a service used at the other level.

If encryption and/or authentication is provided, the security header segment (S3S or S4S) immediately follows the segment initiating the beginning of this level (GS or ST); the security trailer segment (S3E or S4E) precedes the segment terminating the level (GE or SE). If encryption and/or authentication at both levels is provided and if assurances are used at both levels, the sequence of segments, illustrating these levels, is:

ISA—Interchange Header
GS—Functional Group Header
3S—Security Header Level 1
S3A—Assurance Header Level 1
ST—Transaction Set Header
S4S—Security Header Level 2
S4A—Assurance Header Level 2
(The Transaction Set Segments)
SVA—Security Value Level 2
S4E—Security Trailer Level 2
SE—Transaction Set Trailer
SVA—Security Value (Level 1)
S3E—Security Trailer Level 1
GE—Functional Group Trailer
IEA—Interchange Trailer

For 3070 implementations, if encryption and/or authentication at both levels is provided and if assurances are used at both levels, the sequence of segments, illustrating these levels, is:

ISA—Interchange Header
(Other Groups whether secured or not at Level 1)
GS—Functional Group Header
S1S—Security Header Level 1
(Other Transaction Sets whether secured or not at Level 2)
ST—Transaction Set Header
S2S—Security Header Level 2
(The Transaction Set Segments)
S2A—Security Assurance Level 2
SVA—Assurance Token Level 2
(Other optional S2A-SVA pairs at Level 2
S2E—Security Trailer Level 2
SE—Transaction Set Trailer

(Other Transaction Sets whether secured or not at Level 2)

S1A—Assurance Segment Level 1

SVA—Assurance Token Level 1

(Other optional S1A-SVA pairs at Level 1)

S1E—Security Trailer Level 1

GE—Functional Group Trailer

(Other Functional Groups whether secured or not at Level 1)

IEA—Interchange Trailer

10.6 INTERCHANGE CONTROL, ACKNOWLEDGMENT AND SECURITY SEGMENT SPECIFICATIONS

This section contains the implementation conventions for the:

- Interchange Control Header (ISA), Version/release 004010 (original)
- Interchange Control Header (ISA), Version/release 004010 (with syntax correction)
- Interchange Control Header (ISA), Version/release 004020 and higher
- Interchange Delivery Notice Segment (TA3), Version/release 004020
- Functional Group Header (GS), Version/release 002003 through 003010
- Functional Group Header (GS), Version/releases 003040 through 003070
- Functional Group Header (GS), Version/release 004010
- Functional Group Header (GS), Version/release 004020 and higher
- Security Header Level 1 (S1S), Version/releases 003040 and 003050
- Security Header Level 1 (S1S), Version/releases 003060 and 003070
- Security Header Level 1 (S3S), Version/release 004010
- Assurance Header Level 1(S3A), Version/release 004010
- Security Header Level 2 (S2S), Version/releases 003040 and 003050
- Security Header Level 2 (S2S), Version/releases 003060 and 003070
- Security Header Level 2 (S4S), Version/release 004010
- Security Assurance Level 2 (S2A), Version/releases 003060 and 003070
- Assurance Header Level 2 (S4A), Version/release 004010

- Assurance Token Level 2 (SVA), Version/releases 003060 and 003070
- Security Value Level 2 (SVA), Version/release 004010
- Security Trailer Level 2 (S2E), Version/releases 003060 and 003070
- Security Trailer Level 2 (S4E), Version/release 004010
- Assurance Segment Level 1 (S1A), Version/releases 003060 and 003070
- Assurance Token Level 1 (SVA), Version/releases 003060 and 003070
- Security Value Level 1 (SVA), Version/release 004010
- Security Trailer Level 1 (S1E), Version/releases 003060 and 003070
- Security Trailer Level 1 (S3E), Version/release 004010
- Functional Group Trailer (GE), Version/release 002003-004030
- Interchange Control Trailer (IEA), Version/release 002003-004030